# Polynomial representation of Fermat's Last Theorem

Daniele De Pedis
Istituto Nazionale di Fisica Nucleare - Roma1 - Italy
email: daniele.depedis@roma1.infn.it

**Abstract**

We propose a new approach at Fermat's Last Theorem (FLT) solution: for each FLT equation we associate a polynomial of the same degree. The study of the roots of the polynomial allows us to investigate the FLT validity. This technique, certainly within the reach of Fermat himself, allows us infer that this is the *marvelous proof* that Fermat claimed to have.

Keywords: Fermat Last Theorem, Diophantine equations, polynomial

## 1 Introduction

In 1637 Pierre de Fermat wrote in the margins of a copy of Diophants Arithmetical, the book where he used to write many of his famous theories [1]:

> *"It is impossible to separate a cube into two cubes or a fourth power into two fourth powers or, in general, all the major powers of two as the sum of the same power. I have discovered a truly marvelous proof of this theorem, which can't be contained in the too narrow page margin".*

In other words, the previous expression can be condensed into:
the equation:

$$A^n + B^n = C^n \tag{1}$$

has no solutions, other than trivial ones[1], for any value of $A, B, C, n$ integers and n>2.

The equation (1) is known as Fermat's Last Theorem (FLT). Last, not because it was the last work of Fermat in chronological sense, but because it has remained for over 350 years the Fermat's theorem never solved. In fact, also the same Fermat, although stating the unsolvability of (1) he

[1]The trivial solution is a solution with at least one of the integers A, B and C equal to zero

never provided a complete demonstration (maybe lost) but has left his proof limited only to the case n = 4. In reality, therefore, it would be more correct to talk about Fermat's conjecture.

Today, many mathematicians are of the opinion that Fermat was wrong and that he had not a real full demonstration. Others think that Fermat had such proof, or at least that he had guessed the road, but, as was his custom, he was so listless that such evidence went lost. In any case, as you wish to take a position, the fact remains that for over 350 years all the greatest mathematicians have tried to find such evidence without success.

Only in 1994, after seven years of complete dedication to the problem, Andrew Wiles, who was fascinated by the theorem that as a child dreamed to solve, finally managed to give a demonstration. Since then, we might refer to (1) as Fermat's theorem.

However, Wiles used elements of mathematic and modern algebra [2] that Fermat could not know: the demonstration that Fermat claimed to have, if it were correct, then must be so different.

In this paper we'll try to give our contribution proposing a demonstration of Fermat's Last Theorem using a technique certainly within the reach of Fermat himself, and then infer that this is the *marvelous proof* that Fermat claimed to have. In agreement to the supposed Fermat's knowledge, we'll also avoid using procedure and notations proper of modern algebra.

## 2 First considerations [3][4]

Before to go in deep in the proof, we make some well known[2] considerations relating to (1).

a) According to the usual spoken, to say that Fermat's theorem is true is equivalent to saying that (1) is never verified. Nevertheless, the trivial solution is a true solution that we have to consider as we'll see later.

b) It is sufficient to prove (1) be true for the exponent n = 4 and for every n = odd prime. As mentioned the case of n = 4 was proved directly by Fermat.

c) A, B, C must be such that their Greater Common Divider ($GCD$) is the unit when taken in pairs, i.e.:
$GCD(A,B) = GCD(A,C) = GCD(B,C) = 1$ and also $GCD(A,B,C) = 1$.

d) Important corollary to the previous property is that the three variables $A, B, C$ can't all have the same parity and, moreover, only one can be even following this scheme:

| | A | B | C |
|---|---|---|---|
| 1 | odd | odd | even |
| 2 | odd | even | odd |
| 3 | even | odd | odd |

Tab.1

[2] See [3] pag.2

e) Another important corollary of c) is:
$GCD(A+B, C-A) = 1$
$GCD(A+B, C-B) = 1$
$GCD(C-A, C-B) = 1$

## 3 Demonstration of FLT

Here we consider the case 1 of Tab.1, that is $A$ and $B$ both odd.
The cases 2 and 3 in Tab.1 will be discussed in Appendix A.
Let

$$D = C - A = odd\ integer \tag{2}$$
$$E = C - B = odd\ integer$$

then, by the considerations at previous point e), we have $GCD(D, E) = 1$.
From (1) and (2) we obtain

$$A^n + B^n = (C-D)^n + (C-E)^n = C^n \tag{3}$$

where $n$ = prime number $\geq 3$, then developing the powers of binomials

$$(C-D)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} D^k C^{n-k} = C^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} D^k C^{n-k} \tag{4}$$

$$(C-E)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} E^k C^{n-k} = C^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} E^k C^{n-k} \tag{5}$$

where, for convenience, we have released the first term under the sign of summation. Substituting (4) and (5) in (3) we obtain the fundamental relationship

$$P_{(C,n)} = C^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} \left(D^k + E^k\right) C^{n-k} = 0 \tag{6}$$

The (6) is the expression of a polynomial (that we call *associated polynomial*) in the unknown $C$, complete, of degree n and with integer coefficients. The fundamental theorem of algebra assures us that there are n roots of (6) which can be: separate, (partially) overlapping, integer, irrational or complex conjugates[3].

Whatever the type of roots, what interests us is the existence of possible integer roots of (6), in fact, given any integers $D, E$ and $n$, if we could find

[3]The polynomial in (6) being monic and with all integer coefficients cannot have rational no-integer roots [5]. Moreover, as well as in case of complex roots, the irrational roots must appear in conjugate pairs, that is, if $a + \sqrt{b}$ is an irrational root of (6) then also $a - \sqrt{b}$ is a root, where $a$ and $b$ are integer numbers and $\sqrt{b}$ is irrational. See appendix C

at least one integer solution, other than the trivial one, into full set $\{\Gamma_i\}$ of its roots then, using the relations (2), we could get back $A$ and $B$ and disprove Fermat's Theorem.

In other words, if we can prove that the (6) has no integer solutions in $C$, anyhow chosen $D, E$ and $n$, then we can never disprove the theorem and therefore Fermat was right, that is the (1) has no solution in the ring of integers. Equivalently we can state the following

**Lemma 1** *given any integers D, E, and n such that* $GCD(D,E) = 1$ *and* $n \geq 3$*, showing that (6) does not admit any integer solution, other than the trivial one, for the unknown variable C is equivalent to prove that the Fermat's Last Theorem is true.*

The fundamental theorem of algebra assures us that the polynomial in (6) can be expressed as

$$P_{(C,n)} = \prod_{i=1}^{n} (C - \Gamma_i) = 0 \tag{7}$$

where $\Gamma_i$ are the roots of (6).

In order that (6) and (7) are equal, it is necessary and sufficient that the coefficients of the terms of same degree in $C$ are equal. Expanding (6) and (7) in their terms, we get:

$$\begin{aligned} P_{(C,n)} &= C^n - \binom{n}{1}(D+E)\,C^{n-1} + \binom{n}{2}\left(D^2+E^2\right)C^{n-2} - ... \\ &+ \binom{n}{n-1}\left(D^{n-1}+E^{n-1}\right)C - \binom{n}{n}\left(D^n+E^n\right) = 0 \end{aligned} \tag{6a}$$

$$\begin{aligned} P_{(C,n)} &= \prod_{i=1}^{n}(C-\Gamma_i) = (C-\Gamma_1)(C-\Gamma_2)...(C-\Gamma_{n-1})(C-\Gamma_n) = \\ &= C^n - \left(\sum_{i_1=1}^{n}\Gamma_{i_1}\right)C^{n-1} + \left(\sum_{1\leq i_1<i_2}^{n}\Gamma_{i_1}\Gamma_{i_2}\right)C^{n-2} - ... \\ &+ \left(\sum_{1\leq i_1<i_2<...<i_{n-1}}^{n}\Gamma_{i_1}\Gamma_{i_2}...\Gamma_{i_{n-1}}\right)C - (\Gamma_1\Gamma_2...\Gamma_n) = 0 \end{aligned} \tag{7a}$$

The (7a) shows that the development of (7) leads to an expression which is the sum of terms with decreasing powers in $C$ and whose $(n-k)th$ coefficient is related to the sum of all possible combinations, without repetition, of the n roots taken k-at-a-time.

Equating the coefficients of terms of equal degree in (6a) and (7a), we arrive at the following fundamental system of equations (also known as Viete's formula):

$$\begin{cases} \binom{n}{1}(D+E) = \sum_{i_1=1}^{n}\Gamma_{i_1} = \\ \qquad = \Gamma_1 + (\Gamma_2 + ... + \Gamma_{n-1} + \Gamma_n) \qquad\qquad = \Gamma_1 + t_1 \qquad (8a) \\ \binom{n}{2}\left(D^2+E^2\right) = \sum_{1\le i_1<i_2}^{n}(\Gamma_{i_1}\Gamma_{i_2}) = \\ \qquad = \Gamma_1(\Gamma_2+\Gamma_3+...+\Gamma_n) + \sum_{2\le i_2<i_3}^{n}(\Gamma_{i_2}\Gamma_{i_3}) \;\; = \Gamma_1 t_1 + t_2 \qquad (8b) \\ ..... \\ \binom{n}{n-1}\left(D^{n-1}+E^{n-1}\right) = \sum_{1\le i_1<i_2<...<i_{n-1}}^{n}\left(\Gamma_{i_1}\Gamma_{i_2}...\Gamma_{i_{n-1}}\right) = \\ \qquad = \Gamma_1\left(\sum_{2\le i_2<...<i_{n-1}}^{n}\Gamma_{i_2}\Gamma_{i_3}...\Gamma_{i_{n-1}}\right) + \\ \qquad\quad +\Gamma_2\Gamma_3...\Gamma_{n-1}\Gamma_n \qquad\qquad = \Gamma_1 t_{n-2} + t_{n-1} \;\; (8c) \\ \binom{n}{n}\left(D^n+E^n\right) = \Gamma_1\left(\Gamma_2...\Gamma_{n-1}\Gamma_n\right) \qquad\qquad = \Gamma_1 t_{n-1} \qquad (8d) \end{cases}$$

where, $t_1 = (\Gamma_2 + ... + \Gamma_{n-1} + \Gamma_n)$, $t_2 = \sum_{2\le i_2<i_3}^{n}(\Gamma_{i_2}\Gamma_{i_3}) = (\Gamma_2\Gamma_3 + \cdots + \Gamma_2\Gamma_n + \cdots + \Gamma_{n-1}\Gamma_n)$ and so on, and in particular $t_{n-1} = (\Gamma_2\Gamma_3...\Gamma_{n-1}\Gamma_n)$. Moreover, let, without loss of generality, $\Gamma_1$ be the integer trivial root, we will show that it is the only possible integer root. From equations (8) follows the important

**Lemma 2** *If $D$ and $E$ have the same parity then the terms on the right side of each equation in (8) must have an even integer value.*

We will see that the condition $D$ and $E$ both odd is incompatible to fulfill all the relations (8).

According to Lemma 1, to prove the FLT, we have to show that the associate polynomial admits one, and only one, integer root and it is the

trivial solution[4].

**Proof:** We begin observing that in the equation (6a) all terms, except the first one, contain the even factor $(D^i + E^i)$, therefore, if some integer root exists then it must have an even value.

Now, by Lemma 2, the term on the right side of each equation in the system (8) must be an even integer value, then:

- The case in which any of the $t_i$ is non-integer is obviously ruled out.
- $\Gamma_1$ being an even root of (6a) then also $t_1$ and all the $t_i$ must be even integers[5].
- The left side of equation (8c)[6] can never be divided by 4 (see Appendix B) so, being $\Gamma_1$ and $t_{n-2}$ both even, if $t_{n-1}$ was divisible by 4 then the right side would be a multiple by 4 and therefore also this case is excluded.
- The term $t_{n-1}$ is the product of the (n-1) roots of the equation (6a) and, as already said, they can be even integers, irrational or complex. In these last two cases they must appear as conjugate pairs[7].

Therefore we have the following two cases:

**a)** If all the roots $\Gamma_2, \Gamma_3, \ldots \Gamma_{n-1}, \Gamma_n$ are conjugate pairs (irrational or complex) then, also if they fulfill all the relations (8), by Lemma 1 the FLT is proved because there is no any integer root other than the trivial one $\Gamma_1$.

**b)** If some of the $\Gamma_i$ (i=2, 3, ... n) were integers then they must be even and at least a pair, therefore carrying a factor 4 into equation (8c), but this is ruled out by Appendix B.

This exhausts all possible cases, showing that (6a) does not admit integer solutions, other than the trivial one, for any odd integers D and E and for all $n = odd\ primes$ then, by Lemma 1, the Fermat's Last Theorem is proved.

[4]Here, we impose at the trivial solution only the constraint to be integer. It is straightforward to verify into (6) that cases in which ABC=0 imply $P_{(C,n)} = 0$.

[5]The recursive form of the (8) implies the propagation of the $t_i's$ parity along all the equations. In fact in (8a) $\Gamma_1$ and $t_1$, in order their sum is even, must have the same parity then, in (8b) also $t_2$ must have the $t_1$ parity, and so on. On the other hand, $\Gamma_1$ can not be odd, because otherwise the term $\Gamma_1 t_{n-1}$ in (8d) would also be odd in contradiction with Lemma 2.

[6]The (8c) in general will be the penultimate equation of any system with n=p equations. On the left side of this equation there is always the sum of two even powers (i.e. n-1) of odd terms. On the right side, due to the construction procedure of Viete's formulas, there will be always the sum of terms made by all possible combination, without repetition, of n roots taken at groups of n-1 elements.

[7]See Appendix C

# 4 Conclusions

In previous sections we have demonstrated the validity of FLT for n $\geq$ 3 where $A$ e $B$ are both odd (case 1 in Tab.1).

In Appendix A we show that also in cases in which $A$ and $B$ have opposite parity (cases 2 and 3 in Tab.1) the FLT holds.

In conclusion we have proved the validity of Fermat's Last Theorem by a procedure, without doubt, Fermat himself could known and then we can infer that this is the *marvelous proof*, probably been lost, that he claimed to own. The procedure described in this paper does not allow to prove[8] the case n = 4, then we understand why Fermat was worried to demonstrate it in another way.

We note that Andrew Wiles proved the FLT only indirectly. In fact Wiles proved the validity of the Taniyama-Shimura conjecture that asserts that every elliptic curve must be related to a modular form. Gerhard Frey had previously devised a mechanism that links the FLT to the elliptic equations and thus indirectly to the Taniyama-Shimura conjecture.

The demonstration of FLT presented in this work, as well as to verify the validity of FLT itself, through the mechanism of Frey, allows us to say that the Taniyama-Shimura conjecture is also verified without the use of the demonstration of Wiles.

# A Appendix

Here, we want analyze the cases 2 and 3 in Tab.1, that is $A$ and $B$ having opposite parity. Of course is enough discuss only the case 2, indeed the case 3 can be reported to case 2 exchanging the variables $A$ and $B$.

We start again from relation (1), where now we consider $A = odd$ and $B = even$ and therefore $C = odd$, then

$$A^n + B^n = C^n \qquad or \tag{A1a}$$

$$A^n - C^n = -B^n \tag{A1b}$$

Let define the two variables[9] (similar to $D$ and $E$)

$$F = -B - A = odd\ number \tag{A2a}$$

$$G = -B + C = odd\ number \tag{A2b}$$

[8] See Appendix A

[9] Similar consideration regarding $D$ and $E$ made into "First consideration" paragraph, brings us to conclude that $GCD(F, G) = 1$.

From (A1b), (A2a) and (A2b) we have

$$A^n - C^n = (-B-F)^n - (B+G)^n = -B^n \qquad or \qquad (A3a)$$

$$(B+F)^n + (B+G)^n = B^n \qquad (A3b)$$

**Note**: the step from (A3a) to (A3b), due to the negative signs inside the first parentheses, can be done only if $n$ is an odd number[10].

Developing the powers of binomials in (A3b), we get:

$$(B+F)^n = \sum_{k=0}^{n} \binom{n}{k} F^k B^{n-k} = B^n + \sum_{k=1}^{n} \binom{n}{k} F^k B^{n-k} \qquad (A4)$$

$$(B+G)^n = \sum_{k=0}^{n} \binom{n}{k} G^k B^{n-k} = B^n + \sum_{k=1}^{n} \binom{n}{k} G^k B^{n-k} \qquad (A5)$$

where, for convenience, we have released the first term under the sign of summation. Substituting (A4) and (A5) in (A3b) we obtain the fundamental relationship

$$P_{(B,n)} = B^n + \sum_{k=1}^{n} \binom{n}{k} \left(F^k + G^k\right) B^{n-k} = 0 \qquad (A6)$$

The (A6) is the expression of a polynomial in the unknown $B$ completely equivalent, except the term $(-1)^k$, to the equation (6) then it leads at an equation similar to (6a), that is:

$$\begin{aligned} P_{(B,n)} &= B^n + \binom{n}{1} (F+G) B^{n-1} + \binom{n}{2} \left(F^2 + G^2\right) B^{n-2} + ... \\ &+ \binom{n}{n-1} \left(F^{n-1} + G^{n-1}\right) B + (F^n + G^n) = 0 \end{aligned} \qquad (A6a)$$

Now we can borrow all the considerations done on the "Demonstration of FLT" paragraph, then showing that the equation (A6a) cannot admit integer roots, other than the trivial one, therefore proving that the Fermat's Last Theorem is valid also in the cases 2 and 3 of tab.1.

# B Appendix

**Theorem 1** *Let $X$ and $Y$ two odd positive integers and $n$ even then the quantity $X^n + Y^n$ never is divisible by 4.*

[10] Assuming that the proof given in this paper is actually the *marvelous proof* that Fermat claimed to have, probably been lost, then we understand why he worried to demonstrate by other ways the case n = 4.

**Proof:**
Let n=2, then due to the odd value of $X$, will be either $X \equiv 1 \pmod 4$ or $X \equiv 3 \pmod 4$ , then $X^2 \equiv 1 \pmod 4$ for any odd $X$. Moreover, $X^4 = X^2 X^2 \equiv 1 \pmod 4$ so, by induction, $X^n = X^2 X^{n-2} \equiv 1 \pmod 4$ for any even n and odd $X$.
To conclude then $(X^n + Y^n) \equiv 2 \pmod 4$, therefore never divisible by 4.

# C Appendix

Actually the equations (8a) and (8c) pose strong constraints on the values of roots $\Gamma_j$, indeed:

let $\Gamma_{j>1}$ are irrational or integer numbers, then pose $\Gamma_j = \gamma_j + \delta_j$ (with $j > 1$) , where $\gamma_j$ is the integer part of $\Gamma_j$ and $0 \leq \delta_j < 1$ its decimal irrational part.

So that the sum (8a) is an integer, must be

$$t_1 = \sum_{j=2}^{n} \Gamma_j = \sum_{j=2}^{n} (\gamma_j + \delta_j) = \sum_{j=2}^{n} \gamma_j + \sum_{j=2}^{n} \delta_j \tag{C1}$$

where $\sum_{j=2}^{n} \delta_j$ itself must be either integer or null and $n = \textit{odd prime}$.
In similar way from (8c) we have

$$t_{n-1} = \prod_{j=2}^{n} \Gamma_j = \prod_{j=2}^{n} (\gamma_j + \delta_j) \tag{C2}$$

so that both expressions (C1) and (C2) give integer values, needs that the $\Gamma_j$ have conjugated values at pair[11], i.e.:

[11] We begin by considering only two terms $\Gamma_j$ and $\Gamma_{j+1}$, then we must have (from 8a) $S_j = \Gamma_j + \Gamma_{j+1} = (\gamma_j + \delta_j) + (\gamma_{j+1} + \delta_{j+1}) = \textit{integer}$ therefore will be $\delta_j + \delta_{j+1} = 0$ that is $\delta = \delta_j = -\delta_{j+1}$ and moreover (from 8c)
$M_j = \Gamma_j \Gamma_{j+1} = (\gamma_j + \delta)(\gamma_{j+1} - \delta) = \gamma_j \gamma_{j+1} + (\gamma_{j+1} - \gamma_j)\delta - \delta^2 = k$ with $k = \textit{integer}$ then follows
$\delta = \frac{\gamma_{j+1} - \gamma_j}{2} \pm \frac{\sqrt{(\gamma_{j+1} - \gamma_j)^2 - 4\lambda}}{2}$ where $\lambda = k - \gamma_j \gamma_{j+1}$ then getting the positive sign only

$\Gamma_j = (\gamma_j + \delta) = \gamma_j + \frac{\gamma_{j+1} - \gamma_j}{2} + \frac{\sqrt{(\gamma_{j+1} - \gamma_j)^2 - 4\lambda}}{2} = \alpha_j + \sqrt{\beta_j}$ and

$\Gamma_{j+1} = (\gamma_{j+1} - \delta) = \gamma_{j+1} - \frac{\gamma_{j+1} - \gamma_j}{2} - \frac{\sqrt{(\gamma_{j+1} - \gamma_j)^2 - 4\lambda}}{2} = \alpha_j - \sqrt{\beta_j}$ where

$\alpha_j = \frac{\gamma_j + \gamma_{j+1}}{2}$ and $\beta_j = \left(\frac{\gamma_{j+1} - \gamma_j}{2}\right)^2 - \lambda$ therefore

$S_j = \Gamma_j + \Gamma_{j+1} = 2\alpha_j = \gamma_j + \gamma_{j+1}$
$M_j = \Gamma_j \Gamma_{j+1} = {\alpha_j}^2 - \beta_j = \gamma_j \gamma_{j+1} + \lambda$

Taking in account more terms $\Gamma_i$ (i=4, 6,...n) we obtain similar results where the $\alpha_i$ and $\beta_i$ will be function of the corresponding $\gamma_i$, always taken in pair.

$\Gamma_j = \alpha_j + \sqrt{\beta_j}$
$\Gamma_{j+1} = \alpha_j - \sqrt{\beta_j}$

Where $\alpha_j = \frac{\gamma_j + \gamma_{j+1}}{2}$ and $\beta_j = \left[\frac{\gamma_{j+1} - \gamma_j}{2}\right]^2 - \lambda$ with $\lambda$ a suitable integer and $(j = 2, 4, ...n)$.

## References


[1] Simon Singh - Fermat's Last Theorem , The story of a riddle that confounded the world's great minds for 358 years, London: Fourth Estate Limited, 1997.

[2] A. Wiles - Modular elliptic curves and Fermats Last Theorem, Annals of Math. 141 (1995), 443551.

[3] P. Ribenboim - Fermat Last Theorem For Amateurs, Springer-Verlag, 1999.

[4] P. Ribenboim - 13 Lectures on Fermat's Last Theorem, Springer-Verlag, 1979.

[5] K.T. Leung, I.A.C. Mok, S.N. Suen - Polynomials and equation - Hong Kong University press